

[LETTER D - NOTIFICATION TO CUSTOMER]

[NON-UK]

[OFFER OF IDENTITYWORKS]

Dear [First name]

We recently identified a security misconfiguration of an online portal used for internal administrative purposes by RWH Travel Limited. This has resulted in a small amount of our customer data potentially being accessible through online search engines when using specific search terms. However, there is no evidence of any inappropriate or malicious use of impacted data, so we are notifying you on a precautionary basis.

The customer data in question includes holiday plans and walk information which can include personal details of people travelling with us. We share this information through a password protected system with our Tour Leaders in order to operate our overseas holidays effectively, however we recently found an error in the set-up of this system.

This has now been resolved and external cyber-security experts have confirmed that there is no evidence of any unauthorised or malicious use of the data. No financial data has been impacted and our customer websites and booking system were unaffected. The Information Commissioner's Office (ICO) has also confirmed that no regulatory action will be taken.

Please find further information attached, which we hope will provide some reassurance.

We are very sorry that this incident has occurred. We value the privacy of our customers and we are focused on doing everything possible to maintain your trust so that we can continue to welcome you on one of our walking holidays in the future.

Yours sincerely,

XXXX

RWH Travel Limited

IMPORTANT INFORMATION ABOUT YOUR PERSONAL DATA

Is your data affected?

As a precaution, we are directly contacting the limited number of customers whose data may be affected. The data impacted by the incident includes personal data such as name, date of birth, postal addresses, email addresses and in limited cases passport number with issue and expiry date.

No financial data is involved.

What are we doing to resolve the issue?

We take our Data Protection obligations extremely seriously and have taken steps to mitigate any adverse effects, including: engaging forensic information security experts, implementing heightened security measures and notifying the relevant regulatory authorities, such as the Information Commissioner's Office (the ICO) who has confirmed that no regulatory action will be taken.

We have also strengthened the security of the website specifically to ensure this kind of incident cannot happen again.

Although there is no evidence that your data has actually been used by unauthorised third parties, we are offering you 12 months of identity monitoring services, at no cost to you, from one of the UK's leading global information services company.

We hope that this will give you reassurance and peace of mind.

Your free Experian IdentityWorksSM membership

To help you to monitor your personal data for certain signs of potential identity theft, we are offering you a complimentary 12-month membership to Experian *IdentityWorksSM*.

The service monitors the internet, online social networks and public databases on your behalf every hour of the day. It keeps a look out for your details so that it can immediately detect theft, loss or disclosure of your personal and financial information.

If your information is detected in places it should not be, you will be instantly alerted and given help and advice on what to do next to protect yourself from fraud.

Activating your free Experian IdentityWorksSM membership

Activating your free membership is easy. To do so:

1. Visit the IdentityWorksSM website to get started:

www.globalidworks.com/identity1

2. Click on 'Get Started'
3. Enter your details along with the following activation code:[xxxxxx]
4. Ensure that you sign up for the service by [insert date] (your code expires after this date).

Once your membership is activated, you'll have access to the following features:

- Internet Surveillance: Experian's technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information..
- Fraud remediation tips: Self-help tips are available on your member centre.

Steps you can take to protect your identity

We have no knowledge of any unauthorised use of your data. However, we recommend that you take the following precautionary steps to protect yourself from any attempts at fraud or identity theft:

- Keep an eye out for any unusual correspondence or requests for information over the next few months. If you suspect anything unusual, please contact your bank and follow their advice.
- If you are contacted by anyone asking you for personal data or passwords (such as for your bank account), please be vigilant and take all reasonable steps to check the true identity of the organisation.

Further information

We hope that this letter provides you with all the information you require. However, if you still require assistance, then please contact us by emailing dataprotection@rwhtravel.com we will do everything we can to help you.